**Cyber Security Advisories**

**Date: 30 November 2024**

1. **CMTX-P-112024264 : PlugX Malware Campaign**

Threat Overview

1. Threat Campaign: PLUGX Malware Campaign

PlugX is a Remote Access Trojan (RAT), also known as SOGU, Korplug and Destroy RAT usually written in C. It is widely used by Chinese state-sponsored threat actors. This malware acts as a backdoor, allowing full control over the victim’s machine. Its notable features include the ability to execute commands on the affected machine to perform keylogging, capture screen activity, manage processes and services, etc. Its network protocol can vary between samples, potentially using HTTP, HTTPS, a custom binary protocol over TCP or UDP, and ICMP to communicate with the server. PlugX broadcasts UDP signals to devices on the same subnet as the victim and listens for responses to establish connections with other bots on the local network. The RAT has a previous history of being known for its strong encryption, configuration and persistence techniques using side loading techniques for initial infection with Genuine and trusted executable.

Impacts:

o Data Theft and exfiltration : It can steal sensitive information, including personal data, financial records, and intellectual property, leading to potential identity theft or financial loss.

o System Compromise: The malware can gain unauthorized access to systems, allowing attackers to manipulate or damage files, disrupt operations, and compromise system integrity.

o Espionage: It can be used for spying on individuals or organizations, gathering confidential information, and conducting surveillance without the victim’s knowledge.

2. Threat Type : MALWARE

3. Severity: High

Indicators of Compromise (IOCs)

IP Addresses

45.32.248.110

156.59.223.60

167.179.89.246

1. **CMTX-I-290112024 : Malicious Domains used by Threat Actors**

Malicious domains are websites created with the intent to harm, deceive, or exploit users. These domains can be used in various cyberattacks, including spear-phishing, malware distribution, and email-based fraud.

>> Spear-phishing targets individuals by sending emails with links to malicious domains that mimic legitimate sites. Victims are tricked into providing sensitive information, like login credentials, which attackers steal.

>> Malicious domains can also be used to distribute malware. Attackers may set up a website that appears legitimate but secretly hosts harmful software.

>> Typo-squatting involves registering misspelled domains (e.g., g0v.in for gov.in) to trick users into believing they're on a legitimate site. Attackers use these domains in email-based attacks to send fraudulent messages that appear trustworthy.

Prevention Measures:

>> Network administrator should implement email authentication protocols like SPF, DKIM, and DMARC to help detect and prevent email spoofing.

>> Inculcate the practice of verifying domain names and URLs before clicking on links, especially in emails.

>> Regular training sessions to raise awareness about the tactics used by attackers, such as typo-squatting and spear-phishing.

>> Implement Multi-Factor Authentication to add a layer of security.

- ------------------< Malicious Domain>-------

aadhar.jharkhand.gov.in.2024.es

www.www.ftp.cscgov.info

www.karnataka.gov.inwww.bteresults.net

kerala.gov.in.email

assam.gov.in.holiday

\*.gov.in.2024.es

\*.cscgov.info

\*.gov.inwww.bteresults.net

\*.gov.in.email

\*.gov.in.holiday

- ---</Malicious Domain>----------

1. **CMTX-P112024074 : A critical unauthenticated RCE vulnerability in the Palo Alto PAN-OS management interface**

Threat Overview:

A critical unauthenticated remote command execution vulnerability via the PAN-OS management interface is being reported. It is also shared that threat actors are actively exploiting this vulnerability against the publicly exposed firewall management interfaces. Currently, CVE of the vulnerability is not assigned.

Detection

1. To find your assets that require remediation action, visit the Assets section of Customer Support Portal at https://support.paloaltonetworks.com (Products → Assets → All Assets → Remediation Required).

2. The list of devices with an internet-facing management interface discovered in Palo Alto scans were tagged with PAN-SA-2024-0015. If no such devices are listed, it indicates that scan did not find any devices with internet-facing management interface for your account

Mitigations and Recommendations

• Ensure the management interface is configured according to best practices, including placing it on a dedicated VLAN, allowing only secure communication protocols such as SSH and HTTPS, and utilizing jump servers for access to the management IP. Additionally, restrict access to the management interface to trusted internal IPs to minimize the attack surface. A list of Indicators of Compromise (IOCs) related to the attack campaign is provided in the annexure.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Annexure

CERTIn-Threat Intelligence ID- CMTX-P-112024074

- --------------------------------------------------------------------------------------------------

Indicators of Compromise (IOCs):

136.144.17.\*

173.239.218.251

216.73.162.\*

1. **CMTX-I-993112024 : CrimsonRAT- APT36 campaign**

CrimsonRAT is a remote access trojan (RAT) primarily associated with APT36 (a.k.a. Transparent Tribe). It is a state-sponsored threat group focussing on cyber-espionage, particularly against government, defense, and military targets. CrimsonRAT allows attackers to remotely control infected systems, steal sensitive information, log keystrokes, capture screenshots, and exfiltrate data.

- ----------- < C&C IP>---------

162.218.211.215

- ----------- </C&C IP>---------

1. **CMTX-I-295112024 : Malicious Domains used by Threat Actors**

Malicious domains are websites created with the intent to harm, deceive, or exploit users. These domains can be used in various cyberattacks, including spear-phishing, malware distribution, and email-based fraud.

>> Spear-phishing targets individuals by sending emails with links to malicious domains that mimic legitimate sites. Victims are tricked into providing sensitive information, like login credentials, which attackers steal.

>> Malicious domains can also be used to distribute malware. Attackers may set up a website that appears legitimate but secretly hosts harmful software.

>> Typo-squatting involves registering misspelled domains (e.g., g0v.in for gov.in) to trick users into believing they're on a legitimate site. Attackers use these domains in email-based attacks to send fraudulent messages that appear trustworthy.

Prevention Measures:

>> Network administrator should implement email authentication protocols like SPF, DKIM, and DMARC to help detect and prevent email spoofing.

>> Inculcate the practice of verifying domain names and URLs before clicking on links, especially in emails.

>> Regular training sessions to raise awareness about the tactics used by attackers, such as typo-squatting and spear-phishing.

>> Implement Multi-Factor Authentication to add a layer of security.

- ------------------< Malicious Domain>---------

email.gov.in.indiagov.pw

www.mes.gov.in.recruitment-circulars.mesce.org

ww25.ww25.mahagov.info

ww25.hcicolombo.gov.inwww.pravasiharyanadivas.in

www.www.www.ftp.cscgov.info

\*.indiagov.pw

\*.cscgov.info

\*.mesce.org

- ----------------</Malicious Domain>----------

1. **CMTX-P-112024794 : Cumulative Suspicious Domains--ALERT2**

Alert Brief

A set of malicious domains believed to be used in advanced persistent threat (APT) campaigns targeting critical infrastructure, sensitive data, or high-value assets is listed below:

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

win.twittermisc.com

full.buffkill.com

cdn.agadatacenter.com

kkpdy.com

www.carefreeq.com

find.bbmouseme.com

flash.adobe.com.bbmouseme.com

ntp.bbmouseme.com

mplibfd.casacam.net

aihhss.com

transcom.giize.com

api.imango.ink

mlcorsoft.org

bench-marked.com

llx.whoamis.info

api.coinlib.vip

qmsht.freeddns.org

turkmanmfadate.dns05.com

coolstreetwear.com

h5.microsoftshops.com

twotwo.kkb.tv

api.rootjl.com

amytsui.com

krechlq.remotewebaccess.com

app.roundcubeweb.com

update.roundcubeweb.com

adminmvp.vicp.cc

api.stream-amazon.com

plug.active-microsoft.com

node.securesrvr.io

img.office-w.com

apisecurityservice.com

govamazon.com

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **CMTX-P-112024274 : PlugX Malware Campaign**

Threat Overview

1. Threat Campaign: PLUGX Malware Campaign

PlugX is a Remote Access Trojan (RAT), also known as SOGU, Korplug and Destroy RAT usually written in C. It is widely used by Chinese state-sponsored threat actors. This malware acts as a backdoor, allowing full control over the victim’s machine. Its notable features include the ability to execute commands on the affected machine to perform keylogging, capture screen activity, manage processes and services, etc. Its network protocol can vary between samples, potentially using HTTP, HTTPS, a custom binary protocol over TCP or UDP, and ICMP to communicate with the server. PlugX broadcasts UDP signals to devices on the same subnet as the victim and listens for responses to establish connections with other bots on the local network. The RAT has a previous history of being known for its strong encryption, configuration and persistence techniques using side loading techniques for initial infection with Genuine and trusted executable.

Indicators of Compromise (IOCs)

IP Addresses

185.243.113.179

43.230.9.22

43.230.9.230

1. **CMTX-P-112024284 : SHADOWPAD (POISONPLUG) Malware Campaign**

Threat Overview

1. Threat Campaign: SHADOWPAD (POISONPLUG) Malware Campaign

ShadowPad is a sophisticated malware family that continues to be actively used by threat actors for espionage purposes. Its ability to evade detection and maintain persistence makes it a significant threat to targeted organizations. It is a modular cyber-attack tool used by Chinese linked APT groups (APT41/Barium, APT10/Stone Panda, TONTO Team, APT27/Emissary Panda, APT15, Winnti Group, REDECHO).

The malware has plug-in capabilities along with some other capabilities like self-destruction,can persist registry entries or services, and forward network connections. Social media sites have been used by POISONPLUG to host encoded command and control (C&C) orders.

It is designed to run in two stages; The first stage is a shellcode and second stage acts as an orchestrator for modules responsible for C&C communication, working with the DNS protocol, loading and injecting additional plugins into the memory of other processes.

Indicators of Compromise (IOCs):

IP Addresses :Port

95.179.176.94

1. **CMTX-I-401112024 : ActionRAT Malware- Threat Actor: SideCopy**

Pakistan-based threat actors have been actively targeting Indian government and military officials with a malware variant known as ActionRAT. This malware has been used to steal sensitive information through a combination of malicious techniques and sophisticated spear-phishing campaigns, which aim to trick officials into executing infected attachments. Below are some important details:

Indicators of Compromise (IOCs) associated with this malware is as follows:

- ---------- < C&C IP>------

173.212.252.2

- ---------- </C&C IP>------

1. **CMTX-P-112024074 : PXA Stealer**

Threat Overview

PXA Stealer is a Python-based malware designed to steal sensitive information, such as credentials saved in browsers, financial data, and cookies. The attack begins with phishing emails containing a ZIP attachment that includes a Rust-based loader, obfuscated batch scripts, and a decoy PDF. When the loader is executed, it triggers the batch scripts, which open the decoy PDF and run PowerShell commands. These commands then download additional malicious payloads, including the PXA Stealer (a Python package), from infrastructure controlled by the attackers.

Indicators of Compromise (IOCs):

HASHES:

fdad95329954e0085d992cba78188a26abd718797f4a83347ec402f70fe65269

a9e3f6b9047b5320434bc7b64f4ba6c799d2b6919d41ed32e9815742f3c10194

e689601d502cc0cd8017f9d6953ce7e201b2dad42f679dc33afa673249ea1aa4

782da8904a729971fab86286dd1f44e8de686b7bc66b855079381e1c9e97f6da

7db49da15fd159146fe869d049e030a4ecd0d605a762bea4cc4eb702a6ce9ee6

707004559c8d625f2d4b296ede702def1f9f52cadf4c52dadc41f3077531d04f

bc15114841e39203b4e0f5d2cdeef11cc4eceba99eb0c3074a1c6d7b3968404a

URL

https://tvdseo.com/file/synaptics.zip

https://tvdseo.com/file/PXA/PXA\_PURE\_ENC

https://tvdseo.com/file/PXA/PXA\_BOT

https://tvdseo.com/file/Adonis/AdFnis\_Bot

https://tvdseo.com/file/PXA/PXA\_PURE\_ENC

https://tvdseo.com/file/Adonis/Adonis\_Bot

https://tvdseo.com/file/Adonis/Adonis\_XW\_ENC

https://tvdseo.com/file/Adonis/Adonis\_Bot0

https://tvdseo.com/file/STC/Cookie\_Ext.zip

https://tvdseo.com/file/STC/STC\_XW\_ENC

https://tvdseo.com/file/STC/STC\_PURE.b64

https://tvdseo.com/file/STC/STC\_PUP

https://tvdseo.com/file/STC/STC\_OTO

https://tvdseo.com/file/PXA/Cookie\_Ext.zip

https://tvdseo.com/file/STC/STC\_PURE\_ENC

https://tvdseo.com/file/STC/STC\_BOT

https://tvdseo.com/file/PXA/PXA\_BOT

1. **CMTX-I-281112024 : Malicious Domains used by Threat Actors**

Malicious domains are websites created with the intent to harm, deceive, or exploit users. These domains can be used in various cyberattacks, including spear-phishing, malware distribution, and email-based fraud.

- -----------------< Malicious Domain>----------

gov.in.mesce.org

in.mesce.org

mail.mesce.org

mes.gov.in.mesce.org

webdisk.mesce.org

webmail.mesce.org

www.gov.in.mesce.org

www.in.mesce.org

www.mes.gov.in.mesce.org

mail.dot-gov.info

\*.dot-gov.info

\*.mesce.org

- ----------------</Malicious Domain>----------

1. **CMTX-I-053112024 : Malicious Domains used by Threat Actors**

Malicious domains are websites created with the intent to harm, deceive, or exploit users. These domains can be used in various cyberattacks, including spear-phishing, malware distribution, and email-based fraud.

> Spear-phishing targets individuals by sending emails with links to malicious domains that mimic legitimate sites. Victims are tricked into providing sensitive information, like login credentials, which attackers steal.

> Malicious domains can also be used to distribute malware. Attackers may set up a website that appears legitimate but secretly hosts harmful software.

> Typo-squatting involves registering misspelled domains (e.g., g0v.in for gov.in) to trick users into believing they're on a legitimate site. Attackers use these domains in email-based attacks to send fraudulent messages that appear trustworthy.

Prevention Measures:

> Network administrator should implement email authentication protocols like SPF, DKIM, and DMARC to help detect and prevent email spoofing.

> Inculcate the practice of verifying domain names and URLs before clicking on links, especially in emails.

> Regular training sessions to raise awareness about the tactics used by attackers, such as typo-squatting and spear-phishing.

> Implement Multi-Factor Authentication to add a layer of security.

- ----------< Malicious Domain>-------

certinmail.com

mail-govs.icu

- ----------</Malicious Domain>-------

1. **CMTX-I-257112024 : Malicious Domains used by Threat Actors**

Malicious domains are websites created with the intent to harm, deceive, or exploit users. These domains can be used in various cyberattacks, including spear-phishing, malware distribution, and email-based fraud.

- -----------------< Malicious Domain>----------

www.email.gov.in.indiagov.ws

www.apply.gov.in.edumartpro.com

www.digitalassam-gov.in.net

\*.indiagov.ws

\*.gov.in.edumartpro.com

- ----------------</Malicious Domain>---------

1. **CMTX-P112024994 : Relay server Nodes used by Chinese actors--ALERT11**

A state-sponsored threat actor based in China has been observed using anonymization networks such as HiddenOrbit (RedRelay) and SuperJump, along with relay server nodes, to route their traffic and evade detection. The attackers leveraged active VPS nodes, compromised unpatched routers and IP cameras, to target internet-facing networks and security appliances of strategic interest. In this context, a list of relay server nodes actively used by the attackers has been compiled. The shared IP addresses are associated with small home and office (SoHo) routers and IP camera appliances. Additionally, IP profiling indicates that the attackers have specifically targeted unpatched CISCO RV340 VPN Router and Cyberoam devices.

Indicators of Compromise (IOCs):

- -------------------------------------------------------------------------------------------------------

IP ADDRESSES

103.112.86.112

103.134.44.74

103.149.195.155

103.155.57.58

103.157.122.182

103.172.87.249

103.178.77.25

103.180.39.2

103.186.198.112

103.198.187.23

103.211.36.164

103.241.45.90

103.255.72.214

103.255.72.96

103.61.112.215

103.87.58.120

106.51.82.45

110.226.178.33

111.93.41.70

113.193.24.164

115.247.149.122

117.193.160.165

117.247.229.165

122.176.108.166

122.180.246.217

122.184.112.154

122.187.217.130

122.252.246.56

125.23.63.78

136.232.211.246

136.232.99.234

14.141.255.62

148.113.5.21

182.73.242.204

182.74.138.66

182.75.250.10

183.82.121.4

183.82.122.76

210.212.34.199

223.29.207.74

45.112.55.50

45.248.67.252

49.205.195.162

49.248.140.2

49.248.161.12

49.36.91.83

58.146.96.29

59.90.30.197

59.92.70.178

59.92.71.188

59.96.63.119

60.254.2.27

64.227.158.50

1. **CMTX-P-112024038 : Critical Alert: Helldown Ransomware**

Threat Overview

A new ransomware variant named as Helldown is active in the cyber threat landscape. Helldown initially focused on Windows systems, but it later expanded to Linux and VMware ESX servers. Helldown uses a double-extortion tactic. That means it exfiltrates sensitive information in addition to encrypting the victim's data. It uses secure RSA keys to encrypt files.

Impacts:

- -- File Encryption

- -- Personal Information Loss.

- -- Data Exfiltration

Threat Type: Ransomware

Severity: High

Affected Systems: Windows and Linux

Distribution Methods:

Helldown Ransomware primarily spreads through exploiting known vulnerabilities in network devices, particularly Zyxel firewalls. Besides these Attackers use phishing emails and malicious attachments to trick users into downloading malicious payload.

Preventive Measures:

• Patch management: Regularly patch and update software and operating systems to the latest available versions.

• Properly configure and secure internet-facing network devices, disable unused or unnecessary network ports and protocols on VPN servers/ Email servers and recommended to monitor any anomalous application behaviours [new user creation] and unknown connections in the network traffic.

• Network Segmentation: Divide your network into segments to limit the spread of malware if an infection occurs, helping to contain and control the impact.

• Incident Response Plan: Develop and maintain an incident response plan to address malware infections quickly and effectively and minimize damage.

Response Actions:

• Disconnect Affected Systems: Immediately disconnect the infected system from the network to prevent further spread of the malware. Immediately address any signs of unauthorized access by changing passwords, reviewing access logs, and securing compromised accounts.

• Remove Malicious Files: Use an antivirus or anti-malware tool to scan and remove malicious files. Most security software will allow you to perform a full system scan, identifying and quarantining or deleting threats. A list of recent malware hashes are provided in Annexure.

• Update Antivirus Definitions: Ensure your antivirus software is updated with the latest virus definitions. This can usually be done through the software's update function or by downloading the latest definitions from the vendor’s website.

• Apply Security Updates: Ensure all systems and software are updated with the latest security patches to close any vulnerabilities exploited by the malware.

• Enable Two-Factor Authentication (2FA): Implement 2FA for all sensitive accounts to add an additional layer of security

• Periodic Backups and restoration tests to check the restoration integrity.

• The reference link provided below is a one-stop resource to help organizations reduce the risk of ransomware incidents through best practices to detect, prevent, respond, and recover, including step-by-step approaches to address potential attacks:

[https://www.cisa.gov/resources-tools/resources/stopransomware-guide]https://www.cisa.gov/resources-tools/resources/stopransomware-guide

1. **CMTX-P-112024048 : Earth Kasha Threat Actor Campaign**

Threat Overview

1. Threat Campaign: Earth Kasha Threat Actor

Earth Kasha is a sophisticated cyber threat actor linked to China, active since 2019. They primarily target focusing on government, technology, and academia sectors. Recent campaign include spear-phishing campaigns and exploitation of vulnerabilities in public-facing enterprise applications, notably CVE-2023-27997, CVE-2023-28461, and CVE-2023-45727. Threat actor utilize legitimate Microsoft tools (e.g., csvde.exe, nltest.exe) to gather Active Directory configurations and credentials post-initial access.

Impacts:

Data Exfiltration

2. Severity: High

3. Malware Used:

LODEINFO is a sophisticated malware family serves as a backdoor for accessing compromised systems, leveraging vulnerabilities in public-facing applications to gain initial access.

NOOPDOOR is a complex backdoor malware which utilizes two communication channels with its command and control (C&C) server, known as active and passive modes, and injects itself into legitimate applications through XML or DLL files.

Cobalt Strike is a commercial penetration testing tool increasingly exploited by threat actor groups to establish remote access through vulnerable Microsoft Exchange servers and web shells like China Chopper.

Mirror Stealer credential dumper targeting multiple applications such as browsers (Chrome, Firefox, Edge and Internet Explorer), email clients (Outlook, Thunderbird, Becky, and Live Mail), Group Policy Preferences and SQL Server Management Studio.

Initial Access Methods:

Exploiting public-facing vulnerabilities in applications (such as CVE-2023-28461 (Array AG) and CVE-2023-27997 (FortiOS/FortiProxy), and Spear-phishing emails.

Mitigation and Recommendations

Preventive Measures:

• Patch Management: Regularly update and patch all software, applications, and firmware to mitigate vulnerabilities that Earth Kasha might exploit.

• Email Security: Implement advanced email filtering and educate employees on recognizing phishing attempts to prevent initial access.

• Network Segmentation: Use network segmentation to limit lateral movement within the network and protect sensitive data.

• Access Control: Enforce strict access controls and monitor for unusual activity to prevent unauthorized access.

• Multi-Factor Authentication (MFA): Implement MFA to add an extra layer of security for accessing critical systems.

• Endpoint Protection: Deploy advanced endpoint protection solutions to detect and block malicious activities.

• Incident Response: Establish a comprehensive incident response plan and conduct regular drills.

• Reporting: If any suspicious activity is detected or for further assistance, please contact your cybersecurity team immediately.

Detection Techniques:

• Behavioral Analysis: Monitor for unusual network traffic patterns and behaviors that could indicate the presence of malware like LODEINFO or NOOPDOOR.

• Log Analysis: Regularly review system and application logs for signs of suspicious activity, such as unusual login attempts or data exfiltration.

• Threat Intelligence: Utilize threat intelligence feeds to stay updated on the latest tactics, techniques, and procedures (TTPs) used by Earth Kasha.

• Endpoint Detection and Response (EDR): Implement EDR solutions to detect and respond to advanced threats in real-time.

• Vulnerability Scanning: Conduct regular vulnerability scans to identify and address potential weaknesses in the network.

Response Actions:

• Disconnect Affected Systems: Immediately disconnect the infected system from the network to prevent further spread of the malware.

• Remove Malicious Files: Use an antivirus or anti-malware tool to scan and remove malicious files. Most security software will allow you to perform a full system scan, identifying and quarantining or deleting threats.

• Update Antivirus Definitions: Ensure your antivirus software is updated with the latest virus definitions. This can usually be done through the software's update function or by downloading the latest definitions from the vendor’s website.

Annexure: CERTIn-Threat Intelligence ID- CMTX-P-112024048

Indicators of Compromise (IOCs):

- ----------------------------------------

Domain

ns1.tlsart.com

DGA.hopto.org

DGA.gotdns.ch

DGA.myftp.org

DGA.tw8sl.com

DGA.srmbr.com

Hash

9c681493c81581995e6a48b96411a7004fe77558d7ca863e26398538ad78f385

8574a494425825958c1e978ca7f66a467954fa90c7c898eebac49928519f0eae

87fd4cf002e4d3867462c7a08124cba154750ae78785009a9f213c7479241eef

IP Address

45.76.197.236

- -------------------------------------------

MITRE ATT&CK Enterprise Identifier

T1021 (Remote Services)

T1071 (Application Layer Protocol)

T1133 (External Remote Services)

T1003 (OS Credential Dumping)

T1059 (Command and Scripting Interpreter)

T1041 (Exfiltration Over C2 Channel)

T1074 (Data Staged)

T1016 (System Network Configuration Discovery)

T1555 (Credentials from Password Stores)

T1083 (File and Directory Discovery)

- -------------------------------------------------------------

1. **CMTX-P-112024814 : Cumulative Suspicious Domains--ALERT3**

Alert Brief

A set of malicious domains believed to be used in advanced persistent threat (APT) campaigns targeting critical infrastructure, sensitive data, or high-value assets is listed below:

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

fb-down.club

secure.cloudtechnologiesusa.com

login.msvp-upd.com

msvp-upd.com

www.msvp-upd.com

medicalmob.info

srv.activesetting.com

animallover.wiki

openmusicworkshop.com

digitalboundary.msoutlok.online

sharepoint.msoutlok.online

substrate.msoutlok.online

ns1.wildbuns.com

vscodeapp.com

c2.puppeteering-anonymous.com

download.time-sync.org

aadcdn.msvp-upd.com

cooldatashare.com

www.cooldatashare.com

snifflerr.com

activesetting.com

storage.acrobat-kg.com

pickart.space

netcoreupdate.com

censornit.org

c2c.kddk.online

corpusercontent.com

cert.aliyunwaf.top

hmwtv.com

freshairpurifiers.net

ceilgtedom.dw3322.com

superpitpool.com

southfest.io

reclyclebin.com

hosting-mx-ns-g00gle-com.cloud

tls.sharesoffices.com

uz.sharesoffices.com

vu2006.cdncdncdn.top

safedigit.org

techsupportconnect.com

ispcdn.com

dnsshare.net

createchs.co.in

update.icould.in

srv571940.hstgr.cloud

airbnb.housing-longrent.club

baidu.e3216551.online

cozydatee.com

cpanel.ankaramilliyet.com

ddlpark.com

delivreearpentergenereux.info

ea-nacato.space

eating-bear.com

ebwu.info

expectmailer.com

gpt-plus.shop

housing-longrent.club

lashesbyemmanuella.com

m32.in

mail.differential-marketing.com

meet.homepub.xyz

msoutlok.online

mx2.pipexpresslnc.com

myneighborsglasses.com

navdownload.site

nexcomke.splynx.online

nrqrq.com

ns1.medicalmob.info

ntflx-billreturn.com

privatecloud.linker.team

rays-cma.com

relaxlovelive.com

remote-advantage.com

rs-magic.com

servicecs.xyz

srrmtbv.com

srv02249042.ultasrv.com

telcom360.com

tigapilar.online

totravel.world

trust-android.com

twilight365.xyz

update-accinfo.com

v1.trusdtwallec.com

v1.trustwallen.com

vipmarketing.live

walbridgefinancial.com

www.airbnb.housing-longrent.club

www.servicecs.xyz

airgrupdate.ru

x9.dnsseed.bluematt.me

dnsseed.bluematt.me

ycombinator.serveblog.net

eu.minerpool.pw

bitcoinstats.com

netbill.pk

hackroppachl.ddns.net

bbmouseme.com

back123.brasilia.me

microsoft-font-cdn.aeuxq.eu.org

nccu.bbmouseme.com

maintenance.axs-tech.fr

unifi6.smartaligntech.com

ecoquestpurifiers.com

updatens.ru

eck.giize.com

qxpipeline.com

ru.phantom.avira-vpn.com

rss.anotherslice.com

dcc.outformation.io

dcc2.outformation.io

winterfell.outformation.io

ninebar.net

www.go2web.kz

powersrv.de

similarcams.com

bacloud.info

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **CMTX-I-388112024 : Malicious Domain Typo-Squatting CBI Domain used by Threat Actors**

Malicious domains are websites created with the intent to harm, deceive, or exploit users. These domains can be used in various cyberattacks, including spear-phishing, malware distribution, and email-based fraud.

Recently observed such malicious/fake domains are as follows:

-------------< Malicious Domain>----------

cbigov.site

\*.cbigov.site

-------------</Malicious Domain>-----------

Malicious/fake domains typo-squatting CBI have been observed and reported earlier with details as follows:

Fake/Malicious Domains Alert ID Date

cbigov-in.cc CMTX-I-993042024 04/04/2024

cbigov-in.com CMTX-I-993042024 04/04/2024

cbigov-in.net CMTX-I-993042024 04/04/2024

cbigov-in.site CMTX-I-993042024 04/04/2024

cbins.scigv.in CMTX-I-993042024 04/04/2024

\*.cbigovindia.in CMTX-I-053042024 30/04/2024

\*.cbigovnews.in CMTX-I-053042024 30/04/2024

cbigovindia.in CMTX-I-053042024 30/04/2024

cbigovnews.in CMTX-I-053042024 30/04/2024

in2024.cbigov.news CMTX-I-053042024 30/04/2024

in2024.cbigovindia.in CMTX-I-053042024 30/04/2024

cbigovoffice.in CMTX-I-025052024 01/05/2024

cbigovin.site CMTX-I-808062024 20/06/2024

cbigovin.top CMTX-I-808062024 20/06/2024

cbigovins.top CMTX-I-808062024 20/06/2024

cbigovins.site CMTX-I-911062024 26/06/2024

cbigovln.site CMTX-I-404082024 02/08/2024

cbigov.online CMTX-I-650102024 29/10/2024

Network administrators may take required action against the above malicious domains.

1. **CMTX-P-112024324 : PlugX Malware Campaign**

Threat Overview

1. Threat Campaign: PLUGX Malware Campaign

PlugX is a Remote Access Trojan (RAT), also known as SOGU, Korplug and Destroy RAT usually written in C. It is widely used by Chinese state-sponsored threat actors. This malware acts as a backdoor, allowing full control over the victim’s machine. Its notable features include the ability to execute commands on the affected machine to perform keylogging, capture screen activity, manage processes and services, etc. Its network protocol can vary between samples, potentially using HTTP, HTTPS, a custom binary protocol over TCP or UDP, and ICMP to communicate with the server. PlugX broadcasts UDP signals to devices on the same subnet as the victim and listens for responses to establish connections with other bots on the local network. The RAT has a previous history of being known for its strong encryption, configuration and persistence techniques using side loading techniques for initial infection with Genuine and trusted executable.

Indicators of Compromise (IOCs):

IP Addresses: Port

166.88.35.241

141.98.212.50

1. **CMTX-I-981112024 : Malicious Sub-Domains- Possibly Phishing**

Malicious domains are websites created with the intent to harm, deceive, or exploit users. These domains can be used in various cyberattacks, including spear-phishing, malware distribution, and email-based fraud.

- ---------------< Malicious Sub-Domain>-------------

airports-ecom.gov.in.pagesstudy.com

apaar.education.gov.in.login.ph

bih.gov.in.industries

crsorgi.gov.in.web.lndex.online

gov.in.web.index.php.viewcert.org

gov.inwww.uploadmoon.com

ww25.gov.in.web.lndex.online

ww25.incometaxindiaefilinggov.in

www.crsorgi.gov.in.web.lndex.online

www.punepolice.gov.in.puneparking.com

dc.crsorgi.gov.in.birth.indez.in

- --------------</Malicious Sub-Domain>--------------

1. **CMTX-P-112024904 : PlugX Malware Campaign**

PlugX is a Remote Access Trojan (RAT), also known as SOGU, Korplug and Destroy RAT usually written in C. It is widely used by Chinese state-sponsored threat actors. This malware acts as a backdoor, allowing full control over the victim’s machine. Its notable features include the ability to execute commands on the affected machine to perform keylogging, capture screen activity, manage processes and services, etc. Its network protocol can vary between samples, potentially using HTTP, HTTPS, a custom binary protocol over TCP or UDP, and ICMP to communicate with the server. PlugX broadcasts UDP signals to devices on the same subnet as the victim and listens for responses to establish connections with other bots on the local network. The RAT has a previous history of being known for its strong encryption, configuration and persistence techniques using side loading techniques for initial infection with Genuine and trusted executable.

IP Addresses: Port

108.61.223.127

38.60.200.81

1. **CMTX-P-112024804 : SHADOWPAD (POISONPLUG) Malware Campaign**

Threat Overview

1. Threat Campaign: SHADOWPAD (POISONPLUG) Malware Campaign

ShadowPad is a sophisticated malware family that continues to be actively used by threat actors for espionage purposes. Its ability to evade detection and maintain persistence makes it a significant threat to targeted organizations. It is a modular cyber-attack tool used by Chinese linked APT groups (APT41/Barium, APT10/Stone Panda, TONTO Team, APT27/Emissary Panda, APT15, Winnti Group, REDECHO).

The malware has plug-in capabilities along with some other capabilities like self-destruction,can persist registry entries or services, and forward network connections. Social media sites have been used by POISONPLUG to host encoded command and control (C&C) orders.

It is designed to run in two stages; The first stage is a shellcode and second stage acts as an orchestrator for modules responsible for C&C communication, working with the DNS protocol, loading and injecting additional plugins into the memory of other processes.

Indicators of Compromise (IOCs):

IP Addresses :Port

38.54.57.12

1. **CMTX-I-355112024 : CrimsonRAT- APT36 campaign**

CrimsonRAT is a remote access trojan (RAT) primarily associated with APT36 (a.k.a. Transparent Tribe). It is a state-sponsored threat group focussing on cyber-espionage, particularly against government, defense, and military targets. CrimsonRAT allows attackers to remotely control infected systems, steal sensitive information, log keystrokes, capture screenshots, and exfiltrate data.

- ------------ < C&C>---------

24backups6.com

79.143.181.178

- ------------ </C&C>---------

1. **CMTX-P112024605 : ACTIVE EXPLOITATION OF A CRITICAL FLAW (CVE-2023-28461) AFFECTING ARRAY NETWORK**

ALERT BRIEF:

According to the reports, A "Missing Authentication for Critical Function" vulnerability tracked as CVE-2023-28461 exists in Array Networks AG/vxAG secure access gateways is being exploited widely.

Using a flags attribute in an HTTP header, an attacker can access the SSL VPN gateway's filesystem without requiring authentication. A vulnerable URL might then be used to exploit the product.

Earth Kasha, a China-linked cyber espionage group (also known as MirrorFace) has changed its approach from spearphishing to exploiting flaws in file storage services and enterprise products like SSL-VPNs, such CVE-2023-28461 (Array AG).

Threat Type: Vulnerability

CVE-2023-28461

CVSS SCORE-9.8

Severity: High

Associated Malware Families- MirrorStealer and LODEINFO

Associated Threat Actor- Earth Kasha

Affected Version:

1. Array Networks Array AG Series and vxAG (9.4.0.481 and earlier)

2. The vulnerability has NO impact on AVX, APV, ASF and AG/vxAG (running ArrayOS AG 10.x versions) series products.

3. For Array AG/vxAG series products running ArrayOS AG 9.x versions, attackers may exploit this vulnerability without authentication.

IMPACTS:

1. Unauthorized Access: Attackers can gain unauthorized access to sensitive files and data on the affected devices

2. Remote Code Execution (RCE): The vulnerability allows attackers to execute arbitrary code on the affected devices, potentially leading to complete system compromise

3. Data Exfiltration: Sensitive data can be stolen and exfiltrated to remote servers controlled by the attackers

4. Service Disruption: Exploitation can disrupt essential services, leading to downtime and operational challenges

5. System Compromise: The attacker can gain full control over the affected system, posing a significant threat to the security and integrity of the network

MITIGATIONS AND RECOMMENDATIONS:

1. Apply Security Patches: Update your Array Networks AG and vxAG ArrayOS to version 9.4.0.484 or later, as this patch addresses the vulnerability.

Prioritizing patching this issue by following vendor mitigation instructions is crucial. If mitigations are not practical, product discontinuation may be an option. Unauthorized access and serious system harm could result from ignoring this vulnerability.

2. Disable Vulnerable Features: Temporarily disable functionalities such as Client Security, VPN client automatic upgrades, and Portal User Resource

3. Implement Blacklist Rules: Set up blacklist rules to filter out malicious traffic targeting the vulnerable URLs.

4. Network Segmentation: Segment your network to limit the spread of an attack and protect critical systems.

5. Monitor System Logs: Keep a close eye on system logs to detect any unauthorized access attempts or other suspicious activities

6. Intrusion Detection Systems (IDS): Use IDS to detect and alert on any unusual activities targeting the affected devices

7. Regular Security Audits: Conduct regular security audits and assessments to identify and mitigate vulnerabilities in your network infrastructure.

8. User Education: Train employees on recognizing phishing attempts and following best security practices to reduce the risk of initial access.

1. **CMTX-P112024705 : Chinese APT "Earth Estries" Targeting Critical Infrastructure with New Attack Vectors and New Backdoor Malwares**

Alert Brief:

The Chinese APT group "Earth Estries" (also known as Salt Typhoon, FamousSparrow, and GhostEmperor,) has been active since atleast September, 2023 and has mostly targeted government services and vital industries in the US, Asia-Pacific, Middle East, and South Africa, including telecommunications, technology, consulting, chemical, and transportation industries, as well as government agencies and NGOs.

Earth Estries installs malware and performs long-term espionage by using living-off-the-land binaries for lateral movement within networks and by taking advantage of public-facing server vulnerabilities to gain initial access.

The campaign named "Game of Emperor" has been linked to long-term cyber intrusions targeting sensitive information by using sophisticated attack methods and several backdoors, including GHOSTSPIDER, SNAPPYBEE, MASOL RAT and DEMODEX rootkit

The operations of Earth EstriesAPT group usually coincide with the TTPs of other known Chinese APT groups, suggesting that they may be using shared tools from malware-as-a-service vendors. They also employ a sophisticated C&C infrastructure that is overseen by multiple teams.

Brief description about these backdoor malwares is as follows:

1. GHOSTSPIDER-

GHOSTSPIDER is a sophisticated multi-modular backdoor identified during attacks targeting Southeast Asian telecommunications companies. Key features include:

Modular Design: GHOSTSPIDER can load different modules tailored for specific purposes.

Secure Communication: It communicates with its command and control (C&C) server via a custom protocol secured by Transport Layer Security (TLS).

Long-Term Targeting: The backdoor has been utilized in prolonged attacks against government entities and service providers since at least 2020.

Related Threat Groups: Some tactics used by GHOSTSPIDER overlap with those of other APT groups like FamousSparrow and GhostEmperor, although direct attribution remains uncertain.

C&C Infrastructure: Recent findings include GHOSTSPIDER’s C&C infrastructure linked to potential ransomware operations, indicating its use for both espionage and financial gain

2. SNAPPYBEE

SNAPPYBEE, also known as Deed RAT, is another backdoor deployed by Earth Estries. Its characteristics include:

Deployment: SNAPPYBEE was detected in operations targeting government entities, with specific samples found in compromised systems in October 2024.

Shared Tools: It is considered to be a tool shared among various Chinese APT groups, indicating it may not be exclusive to Earth Estries.

Identification: It was linked to the ZINGDOOR attack chains, showcasing its role in complex cyber-attack scenarios

3. MASOL RAT

MASOL RAT is a cross-platform backdoor that has been linked to Earth Estries with a focus on Southeast Asian government networks. Important points include:

Initial Discovery: MASOL RAT was first identified in 2020 during investigations into government-targeted incidents.

Deployment on Linux: The backdoor has been specifically observed targeting Linux devices within government networks.

Limited Attribution: Although MASOL RAT has been associated with Earth Estries, there is still low confidence in linking it to specific exploits without further evidence

4. DEMODEX ROOTKIT

The DEMODEX rootkit plays a significant role in Earth Estries' cyber strategy, enabling them to conduct extensive and persistent attacks on their targets. The group's advanced methodologies and adaptability highlight the ongoing threat posed by sophisticated APTs in the current cyber landscape.

Continued monitoring and analysis will be essential to understand the full extent of their operations and develop countermeasures against such persistent threats.

Indicators of Compromise (IOCs):

HASHES:

fc3be6917fd37a083646ed4b97ebd2d45734a1e154e69c9c33ab00b0589a09e5

fba149eb5ef063bc6a2b15bd67132ea798919ed36c5acda46ee9b1118b823098

2fd4a49338d79f4caee4a60024bcd5ecb5008f1d5219263655ef49c54d9acdec

16c8afd3b35c76a476851f4994be180f0cd72c7b250e493d3eb8c58619587266

9ba31dc1e701ce8039a9a272ef3d55aa6df66984a322e0d309614a5655e7a85c

25b9fdef3061c7dfea744830774ca0e289dba7c14be85f0d4695d382763b409b

6d64643c044fe534dbb2c1158409138fcded757e550c6f79eada15e69a7865bc

b2b617e62353a672626c13cc7ad81b27f23f91282aad7a3a0db471d84852a9ac

05840de7fa648c41c60844c4e5d53dbb3bc2a5250dcb158a95b77bc0f68fa870

1a38303fb392ccc5a88d236b4f97ed404a89c1617f34b96ed826e7bb7257e296

IPs:

103.91.64.214

165.154.227.192

23.81.41.166

158.247.222.165

172.93.165.14

91.245.253.27

103.75.190.73

45.125.67.144

43.226.126.164

172.93.165.10

193.239.86.168

146.70.79.18

146.70.79.105

205.189.160.3

96.9.211.27

43.226.126.165

139.59.108.43

185.105.1.243

143.198.92.175

139.99.114.108

139.59.236.31

104.194.153.65

DOMAINS:

materialplies.com

news.colourtinctem.com

api.solveblemten.com

esh.hoovernamosong.com

imap.dateupdata.com

pulseathermakf.com

www.infraredsen.com

billing.clothworls.com

helpdesk.stnekpro.com

jasmine.lhousewares.com

private.royalnas.com

telcom.grishamarkovgf8936.workers.dev

1. **CMTX-P-TL-1120243214 : Notable Tunneling Tools leveraged by state sponsored/ ransomware actors**

CERT-In has compiled a list of tunneling tools leveraged by state sponsored/ ransomware actors for due consideration. Details are attached.

File Name: Tunneling\_tools.pdf

SHA256: 4bd00e63596fc657a5de019614c33ec425ccfe5a2c62a465bfb96402b719a2e0

1. **CMTX-I-770112024 : AsyncRAT Malware**

AsyncRAT is a backdoor written in .NET that primarily uses unique binary protocol to communicate over TCP. The backdoor can run shell commands and download plugins, which may be kept in the registry or run immediately in memory. Plugins can add features like file transfer, keylogging, video recording, screenshot capture, and cryptocurrency mining. Additionally, ASYNCRAT provides a plugin that targets login credentials kept by web browsers running on Chromium and Firefox. Once executed, AsyncRAT establishes command-and-control (C2) communication with its server and allows threat actors to remotely control compromised systems.

Recent C&C server IP of malware deployed by this threat actor is as follows:

- ---------- < C&C IP>---------

147.185.221.23

- ---------- </C&C IP>---------

1. **CMTX-I-070112024 : Malicious Domain- Spear-Phishing**

Malicious domains are websites created with the intent to harm, deceive, or exploit users. These domains can be used in various cyberattacks, including spear-phishing, malware distribution, and email-based fraud.

- ---------------< Malicious Domain>-------------

mail-nics.online

- ---------------</Malicious Domain>--------------

1. **CMTX-P-112024394 : PlugX Malware Campaign**

Threat Overview

1. Threat Campaign: PLUGX Malware Campaign

PlugX is a Remote Access Trojan (RAT), also known as SOGU, Korplug and Destroy RAT usually written in C. It is widely used by Chinese state-sponsored threat actors. This malware acts as a backdoor, allowing full control over the victim’s machine. Its notable features include the ability to execute commands on the affected machine to perform keylogging, capture screen activity, manage processes and services, etc. Its network protocol can vary between samples, potentially using HTTP, HTTPS, a custom binary protocol over TCP or UDP, and ICMP to communicate with the server. PlugX broadcasts UDP signals to devices on the same subnet as the victim and listens for responses to establish connections with other bots on the local network. The RAT has a previous history of being known for its strong encryption, configuration and persistence techniques using side loading techniques for initial infection with Genuine and trusted executable.

Indicators of Compromise (IOCs)

IP Addresses

118.107.44.132

103.200.97.189

185.239.226.17

72.18.215.38

203.69.170.86

154.82.85.79

134.122.133.95

103.140.186.181

47.75.177.15

109.123.230.56

118.107.44.133

118.107.44.134

134.122.133.86

1. **CMTX-P-112024404 : SHADOWPAD (POISONPLUG) Malware Campaign**

Threat Overview

1. Threat Campaign: SHADOWPAD (POISONPLUG) Malware Campaign

ShadowPad is a sophisticated malware family that continues to be actively used by threat actors for espionage purposes. Its ability to evade detection and maintain persistence makes it a significant threat to targeted organizations. It is a modular cyber-attack tool used by Chinese linked APT groups (APT41/Barium, APT10/Stone Panda, TONTO Team, APT27/Emissary Panda, APT15, Winnti Group, REDECHO).

The malware has plug-in capabilities along with some other capabilities like self-destruction,can persist registry entries or services, and forward network connections. Social media sites have been used by POISONPLUG to host encoded command and control (C&C) orders.

It is designed to run in two stages; The first stage is a shellcode and second stage acts as an orchestrator for modules responsible for C&C communication, working with the DNS protocol, loading and injecting additional plugins into the memory of other processes.

Indicators of Compromise (IOCs)

IP Addresses

217.69.15.243

45.135.118.131

45.131.179.24

95.179.221.218

199.247.2.134

1. **CMTX-P-112024824 : Cumulative Suspicious Domains--ALERT4**

Alert Brief

A set of malicious domains believed to be used in advanced persistent threat (APT) campaigns targeting critical infrastructure, sensitive data, or high-value assets is listed below:

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

agadatacenter.com

helpwithcart.com

nikkicloudservice.com

college.accesscam.org

mvideo.0156059.com

mircoo.supermirco.us

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*